

KEY FORMING METHOD AND DEVICE

Patent number: JP7121107

Publication date: 1995-05-12

Inventor: MIYAUCHI HIROSHI

Applicant: NIPPON ELECTRIC CO

Classification:

- international: G09C1/00; H04L9/00; H04L9/08; H04L9/10; H04L9/12;
H04L9/30; G09C1/00; H04L9/00; H04L9/08; H04L9/10;
H04L9/12; H04L9/28; (IPC1-7): G09C1/00; H04L9/00;
H04L9/10; H04L9/12

- european:

Application number: JP19930270709 19931028

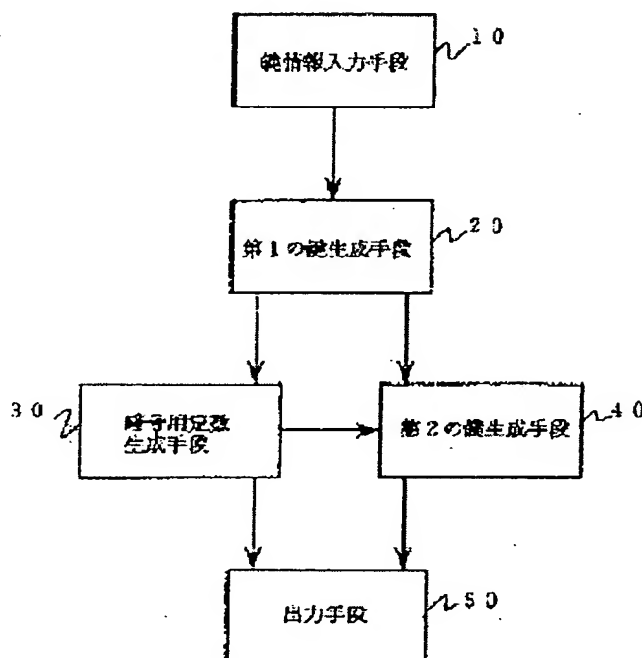
Priority number(s): JP19930270709 19931028

Report a data error here

Abstract of JP7121107

PURPOSE: To enable the utilization of a key arbitrarily desired by a user for either of a privacy key or public key by forming such a constant for a cipher to make a first key as a just key and forming a second key corresponding to the first key.

CONSTITUTION: A key information input means 10 is inputted with the information for forming the first key and sends the inputted key information to a first key forming means 20. The first key forming means 20 forms the first key by subjecting the number obtd. from the numerical value of the key information or the key information to predetermined conversion. A constant forming means 30 for cipher receives the first key from the first key forming means 2 and forms the constant for the cipher in such a manner that the first key is the just key. A second key forming means 40 receives the first key from the first key forming means 20 and the constant for the cipher from the constant forming means 30 for the cipher and forms the second key for the first key. An output means 50 receives the constant for the cipher from the constant forming means 30 for the cipher and the second key from the second key forming means 2 and outputs the received constant and key.



Data supplied from the esp@cenet database - Worldwide



(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 7-121107

(43) 公開日 平成 7 年 (1995) 5 月 12 日

(51) Int. Cl. °	識別記号	庁内整理番号	F I	技術表示箇所
G 0 9 C	1/00	9364-5 L		
H 0 4 L	9/00			
	9/10			
	9/12			
			H 0 4 L	9/00
				Z
審査請求	有	請求項の数 2	O L	(全 4 頁)

(21) 出願番号 特願平5-270709

(22) 出願日 平成 5 年 (1993) 10 月 28 日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 宮内 宏

東京都港区芝五丁目7番1号

日本電気株式

会社内

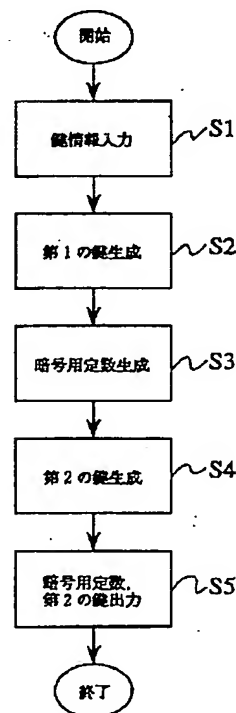
(74) 代理人 弁理士 京本 直樹 (外2名)

(54) 【発明の名称】 鍵生成方法および装置

(57) 【要約】

【目的】 鍵と暗号用定数に成立すべき条件がある公開鍵暗号系を用いる際に、秘密鍵、公開鍵の一方をユーザが指定できる方法および装置を提供する。

【構成】 第1の鍵（秘密鍵または公開鍵）のもととなる情報を入力し（S1）、この情報にあらかじめ定められた変換を施して暗号方式に適合するように第1の鍵を生成する（S2）。次に、この第1の鍵が正当な鍵になるような暗号用定数生成し（S3）、これらの暗号用定数を用いて第1の鍵に対応する第2の鍵を生成し（S4）、暗号用定数と第2の鍵を出力する（S5）。



【特許請求の範囲】

【請求項 1】 公開鍵暗号のための鍵を生成する方法において、第 1 の鍵のもととなる情報を入力し、該情報にあらかじめ定められた交換を施して第 1 の鍵を生成し、この第 1 の鍵が正当な鍵になるような暗号用定数を生成し、前記第 1 の鍵を対応する第 2 の鍵を生成し、前記暗号用定数と第 2 の鍵を出力することを特徴とする公開鍵生成方法。

【請求項 2】 公開鍵暗号のための鍵を生成する装置において、第 1 の鍵のもととなる情報を入力する手段と、該情報を入力して予め定められた変換を施して第 1 の鍵を生成する手段と、第 1 の鍵を入力して該第 1 の鍵が正当な鍵になるような暗号用定数を生成する手段と、暗号用定数および第 1 の鍵を入力し第 1 の鍵に対応する第 2 の鍵を生成する手段と、暗号用定数および第 2 の鍵を出力する手段と、を具備することを特徴とする公開鍵生成装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、鍵と暗号用定数に成立すべき条件がある公開鍵暗号系を用いる際の、秘密鍵、公開鍵、暗号用定数の組を生成する生成方法および生成装置に関する。

【0002】

【従来の技術】 公開鍵暗号系を利用するにあたっては、暗号鍵、復号鍵の他に、定数が必要になる。例えば、代表的な公開鍵暗号である RSA 暗号では、暗号鍵 e 、復号鍵 d 、定数 p 、 q が必要である。ここで、 p 、 q は素数であり、 $n = p \cdot q$ にて算出される n が、暗号に関わるすべての剰余演算の法になる。公開鍵暗号系および RSA 暗号については、池野信一、小山謙二著「現代暗号理論」にくわしく説明されている。

【0003】

【発明が解決しようとする課題】 RSA 暗号では、鍵 k (d または e) と p 、 q のあいだに、 k と $(p-1)(q-1)$ は互いに素という条件が成立することが必須である。従来、 p 、 q を先に決定してこれに適合する e 、 d を作成する方法がとられているが、この方法では e 、 d を自由に選ぶことはできない。

【0004】 このように、鍵と定数が特定の条件を満たさなければならない公開鍵暗号系では、公開鍵、秘密鍵は両方とも特別な意味のない数値となる。このため、ユーザが秘密鍵を記憶するのが困難になり、IC カードなどに保持する必要がある。

【0005】 本発明は、秘密鍵と公開鍵の一方にユーザが任意に選んだ鍵を利用できるように、暗号用手段、公開鍵を生成する方法および装置を提供する。

【0006】

【課題を解決するための手段】 本発明の鍵生成方法は、

第 1 の鍵のもととなる情報を入力し、該情報にあらかじめ定められた変換を施して第 1 の鍵を生成し、この第 1 の鍵が正当な鍵になるような暗号用定数を生成し、前記第 1 の鍵の対応する第 2 の鍵を生成し、前記暗号用定数と第 2 の鍵を出力することを特徴とする。

【0007】 本発明の鍵生成装置、第 1 の鍵のもととなる情報を入力する手段と、該情報を入力して予め定められた変換を施して第 1 の鍵を生成する手段と、第 1 の鍵を入力して該第 1 の鍵が正当な鍵になるような暗号用定数を生成する手段と、暗号用定数および第 1 の鍵を入力して第 1 の鍵に対応する第 2 の鍵を生成する手段と、暗号用定数および第 2 の鍵を出力する手段と、を具備することを特徴とする。

【0008】

【作用】 従来技術では、暗号用定数を先に決定し、これと適合する秘密鍵、公開鍵を生成していたため、秘密鍵として取り得る値に制限があった。しかし、鍵と定数がある条件を満たせばよいのであるから、先に秘密鍵または公開鍵を決定し、これに適合する定数を生成すれば、秘密鍵、公開鍵の一方には任意の鍵を利用することが可能になる。以下では、RSA 暗号を例として説明する。

【0009】 RSA 暗号では、鍵 k (暗号鍵 e および暗号復号鍵 d) と定数として用いる素数 p 、 q の間に k と $(p-1)(q-1)$ は互いに素が成立することが必要である。 p 、 q を先に決めると k として任意の鍵を利用することはできなくなる。しかし、 k を先に決めて、 k と $(p-1)$ 、 $(q-1)$ が素数になるように p 、 q を決定すれば、 k を利用することができる。

【0010】 秘密鍵として、ユーザが決定する数値、文字列を数値化したもの、などを用いれば、暗証番号やパスワードと同様に利用することができて便宜がはかれるのであるが、ここには問題がある。

【0011】 例えば RSA 暗号の場合、 p 、 q は大きな素数であるから、 $(p-1)$ 、 $(q-1)$ はいずれも偶数になる。もしも、ユーザが選んだ数値が偶数であったら、これと $(p-1)$ 、 $(q-1)$ は互いに素になりえない。

【0012】 このように、任意の入力数値、入力文字列をそのまま鍵として利用することは必ずしも可能ではない。そこで、本発明では、入力情報に予め定められた変換を施して鍵を作成する方法をとる。例えば、RSA 暗号の場合には、ユーザが選んだ数値 (または、文字列を数値化したもの) が偶数の場合には 1 を加えるという変換が考えられる。また、 $(p-1)$ 、 $(q-1)$ と互いに素になりやすくするため、入力数値に $2 \times 3 \times 5 \times 7$ のような素数の積を掛けてから 1 を加えるという変換も考えられる。

【0013】 この変換は、入力の数値、文字列に関わらずあらかじめ定めた変換であるから、実際に鍵を利用す

る際も、同様の変換で入力数値、文字列から鍵を生成することが可能である。

【0014】次に、生成された鍵 k が正当な鍵になるように暗号用の定数を生成する。RSA 暗号の場合は、 $(p-1)$ 、 $(q-1)$ と互いに素になるような素数 p 、 q を作成する。このような素数を作成するためには、例えば、大きな乱数を発生し、これが素数であるかどうかと上記の条件を満たすかどうかをチェックする、という手続きを、暗号用定数の条件を満たすものが得られるまで繰り返すという方法が考えられる。

【0015】第1の鍵（暗号鍵または復号鍵） k と暗号用定数を上記のように生成すれば、第2の鍵（復号鍵または暗号鍵）は、通常の方法に従って生成することができる。例えば、RSA 暗号の場合には、 e 、 d の一方と p および q から e 、 d の他方を、

【0016】

【数1】

$$ed \equiv 1 \pmod{L}$$

【0017】に従って作成する。ここで L は $(p-1)$ と $(q-1)$ の最小公倍数である。本発明では、これらの原理を用いて暗号用定数および鍵を生成する。

【0018】

【実施例】図1は第1および第2の発明を説明するための処理の流れを示す図である。図2は第2の発明の実施例の構成を表すブロック図である。以下、これらの図を用いて第1および第2の発明を説明する。

【0019】鍵情報入力手段10は、第1の鍵を作成するための情報を入力する。この情報は、数値であってもよいし、文字列であっても良い。鍵情報入力手段10は、入力した鍵情報を第1の鍵生成手段20へ送る。（図1ステップS1）

第1の鍵生成手段20は、鍵情報入力手段10から鍵情報を受けとり、鍵情報が文字列の場合は、これを数値に変換する。この場合、文字コードをそのまま数値として扱うこともできる。第1の鍵生成手段20は、鍵情報の数値または鍵情報から得られた数に、あらかじめ定め

られた変換をほどこして第1の鍵を生成する。第1の鍵生成手段20は、生成された第1の鍵を暗号用定数生成手段30と第2の鍵生成手段40に送る。（図1ステップS2）

暗号用定数生成手段30は、第1の鍵生成手段20から第1の鍵を受けとり、この第1の鍵が正当な鍵になるように暗号用の定数を生成する。暗号用定数生成手段30は、生成された定数を第2の鍵生成手段40と出力手段50に送る。（図1ステップS3）

10 第2の鍵生成手段40は、第1の鍵生成手段20から第1の鍵を、暗号用定数生成手段30から暗号用定数を受けとり、第1の鍵に対応する第2の鍵を生成する。第2の鍵生成手段40は、生成された第2の鍵を出力手段50に送る。（図1ステップS4）

出力手段50は、暗号用定数生成手段30から暗号用定数を、第2の鍵生成手段40から第2の鍵を受けとり、これらを出力する。（図1ステップS5）

【発明の効果】本発明によれば、公開鍵暗号における秘密鍵、公開鍵のいずれか一方をユーザが指定することができる。秘密鍵をユーザが指定する場合には、ユーザが記憶できる数値または文字列を秘密鍵として用いることができるので、鍵をICカード等の媒体に記録しておく必要がなくなり、コストダウン、利便性の向上がもたらされる。一方、公開鍵をユーザが指定する場合には、そのユーザから容易に導き得る数値や文字列（例えば、名前、ユーザ番号、電話番号など）を公開鍵として用いることができるため、公開鍵簿が不要になるか、簡便なもので済むという効果がえられる。

【図面の簡単な説明】

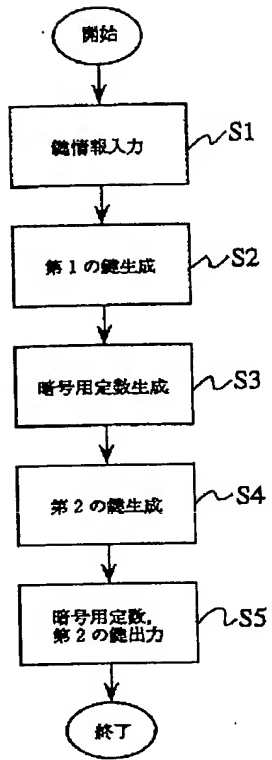
20 【図1】第1および第2の発明の処理の流れを示す図。

【図2】第2の発明のブロック図である。

【符号の説明】

- 10 鍵情報入力手段
- 20 第1の鍵生成手段
- 30 暗号用定数生成手段
- 40 第2の鍵生成手段
- 50 出力手段

【図 1】



【図 2】

